

CLAIMS

What is claimed is:

- 1 1. A method for scanning data read from storage, comprising:
 - 2 a) receiving a request for data saved in storage from a central processing unit;
 - 3 b) scanning the requested data; and
 - 4 c) transmitting the data from the storage to the central processing unit if
 - 5 malicious code is not found in the data during the scanning.
- 1 2. The method as recited in claim 1, wherein the storage is selected from the
2 group consisting of a hard drive, compact disc-read only memory (CD-
3 ROM), and a floppy disk.
- 1 3. The method as recited in claim 1, wherein the scanning is performed by a
2 scanning module coupled to a storage subsystem controller.
- 1 4. The method as recited in claim 3, wherein the storage subsystem controller is
2 coupled to a storage driver which is coupled to the central processing unit.
- 1 5. The method as recited in claim 3, wherein the storage subsystem controller is
2 coupled to the storage.
- 1 6. The method as recited in claim 3, wherein the scanning module includes
2 software.
- 1 7. The method as recited in claim 3, wherein the scanning module includes
2 hardware.

- 1 8. The method as recited in claim 3, and further comprising allowing a user to
2 disable the scanning module.
- 1 9. The method as recited in claim 8, wherein data is precluded from being
2 transmitted from the storage to the central processing unit upon the disabling
3 of the scanning module.
- 1 10. The method as recited in claim 1, and further comprising executing an event
2 based on results of the scanning.
- 1 11. The method as recited in claim 10, wherein the event includes an alert.
- 1 12. The method as recited in claim 10, and further comprising disabling the
2 scanning module in response to the event.
- 1 13. The method as recited in claim 12, wherein data is precluded from being
2 transmitted from the storage to the central processing unit upon the disabling
3 of the scanning module.
- 1 14. The method as recited in claim 1, wherein the scanning includes content
2 scanning.
- 1 15. The method as recited in claim 1, wherein the scanning includes virus
2 scanning.
- 1 16. The method as recited in claim 1, wherein the storage is accessible via a
2 network.
- 1 17. A computer program product for scanning data read from storage,
2 comprising:

- 3 a) computer code for receiving a request for data saved in storage from a central
4 processing unit;
5 b) computer code for scanning the requested data; and
6 c) computer code for transmitting the data from the storage to the central
7 processing unit if malicious code is not found in the data during the scanning.

1 18. The computer program product as recited in claim 17, wherein the storage is
2 selected from the group consisting of a hard drive, compact disc-read only
3 memory (CD-ROM), and a floppy disk.

1 19. The computer program product as recited in claim 17, wherein the scanning
2 is performed by a scanning module coupled to a storage subsystem
3 controller.

1 20. The computer program product as recited in claim 19, wherein the storage
2 subsystem controller is coupled to a storage driver which is coupled to the
3 central processing unit.

1 21. The computer program product as recited in claim 19, wherein the storage
2 subsystem controller is coupled to the storage.

1 22. The computer program product as recited in claim 19, wherein the scanning
2 module includes software.

1 23. The computer program product as recited in claim 19, wherein the scanning
2 module includes hardware.

1 24. The computer program product as recited in claim 19, and further comprising
2 computer code for allowing a user to disable the scanning module.

- 1 25. The computer program product as recited in claim 24, wherein data is
2 precluded from being transmitted from the storage to the central processing
3 unit upon the disabling of the scanning module.
- 1 26. The computer program product as recited in claim 19, and further comprising
2 computer code for executing an event based on results of the scanning.
- 1 27. The computer program product as recited in claim 26, wherein the event
2 includes an alert.
- 1 28. The computer program product as recited in claim 26, and further comprising
2 computer code for disabling the scanning module in response to the event.
- 1 29. The computer program product as recited in claim 28, wherein data is
2 precluded from being transmitted from the storage to the central processing
3 unit upon the disabling of the scanning module.
- 1 30. The computer program product as recited in claim 17, wherein the scanning
2 includes content scanning.
- 1 31. The computer program product as recited in claim 17, wherein the scanning
2 includes virus scanning.
- 1 32. The computer program product as recited in claim 17, wherein the storage is
2 accessible via a network.
- 1 33. A method for scanning data written to storage, comprising:
2 a) receiving a request for data to be written in storage, the request being
3 received from a central processing unit;
4 b) scanning the data; and

- 5 c) writing the data to the storage if malicious code is not found in the data
6 during the scanning.

- 1 34. A computer program product for scanning data written to storage,
2 comprising:
3 a) computer code for receiving a request for data to be written in storage, the
4 request being received from a central processing unit;
5 b) computer code for scanning the data; and
6 c) computer code for writing the data to the storage if malicious code is not
7 found in the data during the scanning.

- 1 35. A system for scanning data read from storage, comprising:
2 a) storage for saving data therein;
3 b) a storage subsystem controller coupled to the storage for controlling access to
4 the data saved therein;
5 c) a central processing unit coupled to the storage subsystem controller for
6 issuing read requests for reading the data saved therein for processing
7 purposes, and write requests for writing data to the storage;
8 d) a scanning module coupled to the central processing unit and the storage
9 subsystem controller, the scanning module adapted for identifying the
10 requests from the central processing unit, and scanning the data in response
11 to the requests; and
12 e) an event manager module coupled to the scanning module and the central
13 processing unit, the event manager module adapted for receiving results of
14 the scanning from the scanning module, the event manager module adapted
15 to execute an event based on the results of the scanning;
16 f) wherein the central processing units is conditionally allowed to read the data
17 saved in the storage and write data to the storage based on the results of the
18 scanning.

- 1 36. The system as recited in claim 35, wherein the scanning module is coupled to
2 the storage subsystem controller via a bus.
- 1 37. The system as recited in claim 35, wherein the scanning module is directly
2 coupled to the storage subsystem controller.
- 1 38. The system as recited in claim 35, wherein the scanning module is coupled to
2 the storage subsystem controller via a storage driver.
- 1 39. A system for scanning data read from storage, comprising:
2 a) means for saving data therein;
3 b) means for controlling access to the data saved therein;
4 c) means for issuing read requests for reading the data saved therein for
5 processing purposes and write requests for writing data to the storage;
6 d) means for identifying the requests from the central processing unit, and
7 scanning the data in response to the requests; and
8 e) means for receiving results of the scanning from the scanning module, the
9 event manager module adapted to execute an event based on the results of the
10 scanning;
11 f) wherein the central processing units is conditionally allowed to read the data
12 saved in the storage and write data to the storage based on the results of the
13 scanning.